

JOHN HUBER, United States Attorney (#7226)
Aaron Flater, Assistant United States Attorney (#9458)
Attorneys for the United States of America
111 South Main Street, #1800
Salt Lake City, Utah 84111
Telephone: (801)524-5682
Aaron.Flater@usdoj.gov

FILED IN UNITED STATES DISTRICT
COURT, DISTRICT OF UTAH
JUL 31 2019
BY D. MARK JONES, CLERK
DEPUTY CLERK

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

IN THE MATTER OF THE SEARCH OF
ELECTRONIC DEVICES DESCRIBED IN
ATTACHMENT A OF THIS DOCUMENT,
CURRENTLY LOCATED AT 2975 S. Decker
Lake Drive, West Valley City, Utah 84119

Case No. 2:19-mj-536-DBP

AFFIDAVIT

I, Ryan Weir, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a sworn special agent for Homeland Security Investigations (HSI) and have been so for approximately nine years. Before being employed with HSI, I was a special agent with the United States Secret Service (USSS) for approximately five years. As a special agent of the USSS, I attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. As a special agent with HSI, I have attended the

Immigration and Customs Enforcement Special Agent Training school at the Federal Law Enforcement Training Center in Glynco, Georgia. As part of my regular duties with HSI, I investigate offenses relating to violations involving Title 18, United States Code, 545 and 542, Title 21, United States Code, 841, 846 and 952.

3. The applied-for warrant would authorize the forensic examination of the “Devices” for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

1. On or about 04/20/2018, CBP in Chicago inspected a mail parcel that was being mailed to Justin RISLEY at 636 Angie Circle, Midvale, Utah - a former residence of RISLEY and current residence of his mother. The parcel was being mailed from the Netherlands. The parcel contained 53 pills that tested positive for Ecstasy, a Schedule I controlled substance. The parcel also contained six (6) grams of MDMA powder.

2. On or about 09/19/2016, CBP officers at the John F. Kennedy International Airport (JFK) International Mail Facility inspected a mail parcel that was being mailed to Justin RISLEY at 636 Angie Circle, Midvale, Utah - a former residence of RISLEY and current residence of his mother. The parcel was being mailed from Germany. The parcel contained 220 orange pills with “WB” imprinted on them that tested positive for MDMA/Ecstasy.

3. On or about 06/10/2016, CBP officers in Chicago inspected a mail parcel that was being mailed to Justin RISLEY at 636 Angie Circle, Midvale, Utah - a former residence of RISLEY

and current residence of his mother. The parcel was being mailed from The Netherlands. The parcel contained 52 tablets that tested positive for MDMA, a Schedule I controlled substance.

4. On or about 11/24/2015, CBP officers in Chicago inspected a mail parcel that was being mailed to Justin RISLEY at 8279 S. Lance Street, Apt. # 10, Midvale, Utah – a former residence of RISLEY. The parcel was being mailed from The Netherlands. The parcel contained 10 tablets that tested positive for Ecstasy.

5. On or about June 25, 2019, United States Customs and Border Protection (CBP) Officers in the John F. Kennedy International Airport (JFK) International Mail Facility selected an inbound parcel bearing tracking number LB744980328DE from Germany for intensive examination. The package was addressed to the following consignee: Justin Risley, 51 Millpond Stansbury Park, Utah 84074-9605. The declared contents on the parcel was manifested as “1x cosmetics”. Using their border search authority, specifically 19 U.S.C. 482, 1467, 1581 and 1582, CBP officers opened the parcel and found it to contain a clear shrink-wrapped bag containing pills secreted within a paper envelope. Presumptive Drug Tests (PDT) were conducted by CBP of the discovered pill substances. Subsequent PDT field tests were conducted on the discovered substance in the following sequence: 1-PDT #180 Test Kit showed positive for the presence of general narcotic compounds; 2-PDT #101 Test Kit showed positive for the presence of amphetamine; and 3-PDT #164 Test Kit showed positive for the presence of MDMA/Ecstasy. The total weight of the pills was approximately 205 grams.

6. MDMA is a Schedule I drug under the Controlled Substances Act. MDMA is a synthetic chemical made in labs. MDMA found in the U.S. is primarily manufactured in and smuggled across our borders from clandestine laboratories in foreign countries including European countries.

7. On July 03, 2019, acting in an undercover capacity as a U.S. Postal Mail Carrier, United States Postal Inspector (USPIS) Dimick delivered the parcel containing 205 grams of MDMA that was seized by CBP on or about June 25, 2019, to Justin RISLEY's residence located at 51 Millpond Stansbury Park, Utah 84074. When USPIS Dimick knocked on the front door to the residence, Katherine Risley answered the door. USPIS Dimick stated he had a parcel addressed to Justin and asked Katherine Risley if she knew him and Risley replied he was her husband. Katherine Risley then took possession of the parcel and took inside the residence at 51 Millpond Stansbury Park, Utah 84074.

8. On July 03, 2019, a short time after Risley accepted the parcel containing MDMA and took it inside the residence, agents with HSI and the Tooele County Sheriff's Office executed a federal anticipatory search warrant at Risley's residence. During the search of Risley's residence agents found and seized items of evidentiary value including marijuana, methamphetamine, oxycodone, psychedelic mushroom spores, digital scale, empty pills capsules and electronic devices including a Mophie external hard drive, iPhone cellular telephone, an LG cellular telephone and a Verbatim external thumb drive belonging to Justin and or Katherine Risley.

9. During interviews conducted by your affiant and Detective Reyes on July 3, 2019, both Katherine and Justin Risley stated that they were the only ones who resided at the residence on Millpond but denied any knowledge of the methamphetamine that was recovered by investigators in their master bathroom. When questioned about the psychedelic mushroom spores, Justin Risley stated that the company he ordered them from sent the wrong product and that they had ordered edible mushrooms because he and his wife like to garden. When questioned about the oxycodone, Justin stated that they may have belonged to Katherine's grandmother, but acknowledged that her grandmother did not reside with them. Risley denied ordering the MDMA that was intercepted by CBP and further denied any knowledge of the parcel. As previously mentioned in this affidavit in paragraphs 1-4 there have been other parcels containing MDMA/Ecstasy that were intercepted and seized by CBP with Justin Risley as the listed consignee going to his known previous addresses. When questioned about those previous seizures, Justin Risley denied any knowledge of those parcels containing MDMA/Ecstasy.

KNOWLEDGE BASED ON TRAINING AND EXPERIENCE

10. Based upon my training and experience, and conversations with, and training from, other officers and agents involved in narcotics and money laundering investigations, I know the following:

11. Traffickers of controlled substances, and those who assist them, maintain and tend to retain accounts or records of their drug trafficking activities, including lists of drug quantities and money owed, telephone records including contact names and numbers, photographs, and similar records of evidentiary value. These items are generally kept in locations where drug

traffickers believe their property is secure and will remain undetected from law enforcement, such as inside their homes or stored in vehicles and on their electronic devices.

12. Traffickers of controlled substances commonly maintain addresses, contact names and numbers and email addresses, order history, which reflect names, addresses, and/or telephone numbers of their suppliers, customers and associates in the trafficking organization and it is common to find drug traffickers keeping records of said associates in cellular telephones and other electronic devices including external memory devices. Traffickers often maintain cellular telephones for ready access to their clientele and to maintain their ongoing illegal drug distribution business.

13. Illegal drug traffickers sometimes take or cause to be taken photographs and/or video recordings of themselves, their associates, their property, and their illegal product, or have photo or video security systems that record images from their homes or property. These individuals usually maintain these photographs and recordings in their possession, at their premises, or at some other safe place, including their electronic devices.

14. Illegal drug trafficking is a continuing activity over months and even years. Illegal drug traffickers will repeatedly obtain and distribute controlled substances on a somewhat regular basis, much as any distributor of a legitimate commodity would purchase stock for sale and, similarly, such drug traffickers will have an "inventory" which will fluctuate in size depending upon various factors to include the demand and supply for the product. I would expect the trafficker to keep records of his illegal activities for a period of time extending beyond the time during which he actually possesses illegal controlled substances, in order to maintain contact with his criminal associates for future drug transactions, and so that he can have records of prior

transactions for which, for example, he might still be owed money, or might owe someone else money. These records are often created in code.

15. Drug dealers use cellular telephones and other electronic devices including computers and external media devices as a tool or instrumentality in committing their criminal activity to include the purchase of narcotics on the Internet and to store important data regarding their criminal activity. They use the electronic devices to maintain contact with their suppliers, distributors, and customers. They use media storage devices to maintain records of their criminal activity including contacts, where and who they order narcotics from, ledgers, payments made and or received. Since cellular phone use became widespread, every drug dealer I have contacted has used one or more cellular telephones for his or her drug business. Based on my training and experience, the data maintained in a cellular telephone used by a drug dealer is evidence of a crime or crimes. This data includes the following:

16. The assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by co-conspirators, to identify other telephones used by the same subscriber or purchased as part of a package, and to confirm if the telephone was contacted by a cooperating source.

17. Stored text messages are important evidence. Agents can identify both drug associates and friends of the user who likely have helpful information about the user, his location, and his activities.

18. Photographs on a cellular telephone are evidence because they help identify the user, either through his or her own picture, or through pictures of friends, family, and associates that can identify the user. Pictures also identify associates likely to be members of the drug trafficking organization. Also, digital photos often have “geocode” information embedded in them. Geocode information is typically the longitude and latitude where the photo was taken. Showing where the photo was taken can have evidentiary value. This location information is helpful because, for example, it can show where coconspirators meet, where they travel, and where assets might be located

19. Stored address records are important evidence because they show the user’s close associates and family members, and they contain names and nicknames connected to phone numbers that can be used to identify suspects.

20. The Devices are currently in storage at 2975 S. Decker Lake Drive, West Valley City, Utah. In my training and experience, I know that the Devices have been stored in a manner in which its’ contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. The “devices” (iPhone, LG cellphone, Mophie external hard drive and Verbatim external thumb drive): An iPhone and LG cellphone are wireless telephones (or mobile telephone, or cellular telephone) and are handheld wireless devices used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to

photographs or videos. The iPhone and LG cellphone indicated in this affidavit contain digital cameras.

28. Based on my training, experience, and research, I know that the mobile communication devices have capabilities that allow it to serve as a wireless telephone, text messaging, address book, daily calendar of events, digital camera, email communications and Internet searches. Based on my training and experience, and research, I know that the external media storage devices are used by those involved in narcotics distribution to maintain records of their criminal activity including “customer” lists, lists of suppliers, type and use of payment made. Additionally, in my training and experience, examining data stored on devices of these types can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

//

//

//

//

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant

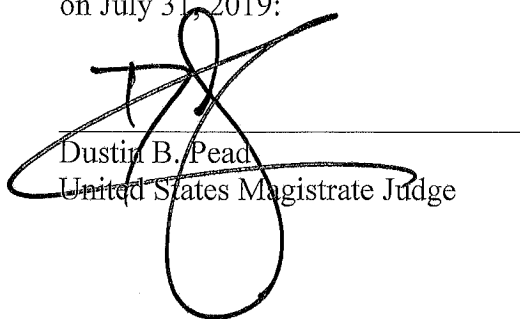
authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'RYAN WEIR', written over a horizontal line.

RYAN WEIR
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me
on July 31, 2019:

A large, stylized handwritten signature in black ink, written over a horizontal line.

Dustin B. Peard
United States Magistrate Judge

ATTACHMENT A

THE DEVICES TO BE SEARCHED

The property to be searched consists of the following:

- a. A white iPhone IMEI: 354453060515668
- b. A black Verbatim thumb drive
- c. A silver LG cellphone
- d. A green and silver colored Mophie external hard drive

These items will be referred to as the “Devices.” The Devices are currently located at 2975 S. Decker Lake Drive, West Valley City, Utah.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

THE INFORMATION TO BE SEIZED

1. All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. 542 and 545 and Title 21 U.S.C. Sec. 841, 846 and 952 that involve Justin RISLEY, including:

- a. lists of customers, and related identifying information;
- b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. any information related to the sources of narcotics (including names, addresses, phone numbers, websites or any other identifying information);
- d. any information recording Justin RISLEY's schedule or travel;
- e. all recordings both audio and visual indicating possession, storage, or trafficking of narcotics (to include EXIF data associated with visual recordings which can provide evidentiary dates and locations associated with the recordings);
- f. all communications to include but not limited to email, text or media messages, instant messaging, or messaging applications utilizing the Internet.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords;

3. Any other fruits or instrumentalities of the crimes of Smuggling and Conspiracy to Distribute narcotics including MDMA, cocaine, marijuana and Aiding and Abetting.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.